UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/705,782	11/10/2003	Andrew Dellow	851963.414	4386

38106 7590 02/18/2010

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVENUE, SUITE 5400
SEATTLE, WA 98104-7092

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
02/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/705,782	DELLOW ET AL.	
	Examiner	Art Unit	
	SUMAN DEBNATH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending in this application.

2. The text of these sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Claim Rejections - 35 USC § 103

1. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mills (Patent No.: US 6,311,204 B1) and further in view of Ducharme (Patent No.: US 7,165,180 B1).

2. As to claim 1, a semiconductor integrated circuit, provided as a monolithic circuit, for decryption of broadcast signals, comprising:

Mills discloses an input interface for receipt of received encrypted broadcast signals, a broadcast encrypted common key, and broadcast control data, and an output interface for output of decrypted broadcast signals ("The EMMs may also be used to specify an entitlement time range, or event signaling information such as near video on demand (NVOD)/pay-per-view (PPV) billing credits, return channel access schedules, parental control information or custom application-defined events. A given EMM may contain an encrypted service key which is used to decrypt subsequent ECMs. The service keys are changed at a relatively low rate, typically on the order of days or months. The ECMs are addressed to the decoders 52, 54 and contain encrypted control words (CWs) which are changed at a relatively frequent rate, typically on the

order of seconds. The EMMs and ECMs identified in demux 50 are queued by processor 20 in DRAM 40 for transmission through the smartcard interface 80 to the smartcard. A direct memory access (DMA) technique may be used to implement this transfer. The smartcard stores a secret key for the processing system 10 and uses the secret key to decrypt an encrypted service key and thereby authenticate the EMM information. The decrypted service key is then used to decrypt the encrypted CWs which are supplied to the DVB descrambler 26 for use in decoding portions of an entitled program. Any event EMMs may be transferred to an event queue for processing by the CPU 30." e.g. see, col. 11, lines 9-50; *It should be noted that Mills's invention related to multimedia distribution systems (i.e. broadcasting signal); Mills teaches common keys as service keys;*);

a processing unit arranged to receive encrypted broadcast signals via the input interface, to decrypt the encrypted broadcast signals in accordance with control signals, and to provide decrypted broadcast signals to the output interface ("The decrypted service key is then used to decrypt the encrypted CWs which are supplied to the DVB descrambler 26 for use in decoding portions of an entitled program. Any event EMMs may be transferred to an event queue for processing by the CPU 30." e.g. see, col. 11, lines 9-50);

a first decryption circuit arranged to receive encrypted control signals from the input interface and to decrypt the control signals in accordance with a decrypted common key from a dedicated common key store (("The decrypted service key is then used to decrypt the encrypted CWs which are supplied to the DVB descrambler 26 for

use in decoding portions of an entitled program. Any event EMMs may be transferred to an event queue for processing by the CPU 30." e.g. see, col. 11, lines 9-50; *Mills teaches common keys as service keys; It also should be noted that Mills teaches that service keys are changed at a relatively low rate (i.e. typically on the order of days or months), anyone with ordinary skill in the art would understand that the service keys are temporarily stored in the receiving side since it's changes in low rate (i.e. there is no need for keep sending the same service keys over and over again*); and

a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store ("The smartcard stores a secret key for the processing system 10 and uses the secret key to decrypt an encrypted service key and thereby authenticate the EMM information.");

Although Mills discloses receiving common key in encrypted form by broadcast signal (e.g. col. 11, lines 9-50), Mills may not explicitly disclose that the common key is stored in decrypted form in an integrated circuit, whereby the circuit is arranged such that the only route to placing a common key in the common key store is to receive in encrypted from for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key, neither may not explicitly disclose a secret key store is located in the integrated circuit or having common key store and

secret key store in a monolithic device which configured to store common key and secret key.

However, Ducharme discloses the common key is stored in decrypted form in an integrated circuit (col. 2, lines 18-50, col. 3, lines 5-61, col. 4, lines 35-47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65; *it should be noted that Ducharme discloses a encryption key register 130 (FIG. 1) which teaches the concept of having a common key store in an integrated circuit and/or in a monolithic device*), whereby the circuit is arranged such that the only route to placing a common key in the common key store is to receive in encrypted from for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus (col. 2, lines 18-50, col. 3, lines 5-61, col. 4, lines 35-47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65), and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key, neither may not explicitly disclose a secret key store is located in the integrated circuit or having common key store and secret key store in a monolithic device which configured to store common key and secret key (col. 2, lines 18-50, col. 3, lines 5-65, col. 4, lines 35-47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Mills as taught by Ducharme in order to store keys in a secure manner, thus third party access to the keys are prevented (i.e. see Ducharme, col. 4, lines 19-32).

3. As to claims 10, 13, 16 and 19, these are rejected using the similar rationale as for the rejection of claim 1.

4. As to claim 2, the combinations of Mills and Ducharme disclose wherein the first decryption circuit and second decryption circuit are formed in a common circuit (Ducharme: col. 2, lines 18-50, col. 3, lines 5-65, col. 4, lines 35-47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65; *which describes a monolithic device*).

5. As to claim 3, the combinations of Mills and Ducharme disclose wherein at least one of the first decryption circuit and the second decryption circuit comprises an AES circuit (Ducharme: col. 3, lines 54-61).

6. As to claim 4, the combinations of Mills and Ducharme disclose wherein the broadcast signal comprises a digital television signal and the processing unit comprises a DVB circuit (Mills: col. 11, lines 9-50, FIG. 1).

7. As to claim 5, the combinations of Mills and Ducharme disclose wherein the input interface has a separate input for the encrypted common key connected to the decryption circuit (Mills: col. 11, lines 9-50, FIG. 1).

8. As to claim 6, the combinations of Mills and Ducharme disclose wherein the secret key is unique to the semiconductor integrated circuit (Mills: col. 11, lines 30-50).

9. As to claims 14 and 17, these are rejected using the similar rationale as for the rejection of claim 6.

10. As to claim 7, the combinations of Mills and Ducharme disclose wherein the common key store is arranged to store multiple common keys (Ducharme: col. 2, lines 18-50, col. 3, lines 5-65, col. 4, lines 35-47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65).

11. As to claim 11, 15, 18 and 20, these are rejected using the same rationale as for the rejection of claim 7.

12. As to claim 8, the combinations of Mills and Ducharme disclose a television decoder comprising the semiconductor integrated circuit of claim 1 (Mills: FIG. 1, col. 11, 9-50).

13. As to claim 9, it is rejected using the similar rationale as for the rejection of claim 1.

14. As to claim 12, the combinations of Mills and Ducharme disclose wherein the decryption device is formed as a single semiconductor integrated circuit having an input interface for receipt of encrypted broadcast signals, encrypted control signals, and

encrypted common keys, and an output interface for output of decrypted broadcast signals (Mills: FIG. 1, col. 11, 9-50).

15. As to claim 21, it is rejected using the same rationale as for the rejection of claim 12.

16. **Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the Applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Response to Arguments

17. Applicant's arguments filed November 17th, 2009 have been fully considered but they are not persuasive.

18. Applicant argues that: "The Ducharme reference, also relied upon by the Examiner in combination with Mills, describes a monolithic device that can store a key in

a secure way, but it says nothing as to how the key store can be populated, much less whether multiple keys can be stored therein that are provided by broadcasts.

Examiner maintains that Ducharme teaches the common key is stored in decrypted form in an integrated circuit (col. 2, lines 18-50, col. 3, lines 5-61, col. 4, lines 35-47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65; *it should be noted that Ducharme discloses a encryption key register 130 (FIG. 1) which teaches the concept of having a common key store in an integrated circuit and/or in a monolithic device*). It should be noted that a key register is a key store which can hold multiple keys. Furthermore, storing keys either in encrypted or decrypted form is well known in the art for long time, which couldn't be novelty of the invention. Applicant also should note that Mills teaches other aspect of claimed invention such as how the keys are broadcasted (e.g. see, e.g. col. 11, lines 9-50).

19. Applicant argues that: "Mills does not teach or suggest a number of features recited in claim 1, including providing all of the circuit components on a monolithic circuit, storing a secret key on the monolithic circuit that is used to decrypt encrypted control words and to provide control signals to a processing unit that decrypts the broadcast signal. Mills also doesn't teach or suggest a dedicated common key store in the integrated circuit that then provides the decrypted common key to the processing unit.

Applicant should note that Mills teaches the main concept of the Applicant's invention. Examiner asserts that Mills may teaches dedicated key store ("The decrypted

service key is then used to decrypt the encrypted CWs which are supplied to the DVB descrambler 26 for use in decoding portions of an entitled program. Any event EMMs may be transferred to an event queue for processing by the CPU 30." e.g. see, col. 11, lines 9-50; *Mills teaches common keys as service keys; It also should be noted that Mills teaches that service keys are changed at a relatively low rate (i.e. typically on the order of days or months), anyone with ordinary skill in the art would understand that the service keys are temporarily stored in the receiving side since it's changes in low rate (i.e. there is no need for keep sending the same service keys over and over again).* However, Examiner also cited Ducharme who teaches the common key is stored in decrypted form in an integrated circuit (col. 2, lines 18-50, col. 3, lines 5-61, col. 4, lines 35-47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65; *it should be noted that Ducharme discloses a encryption key register 130 (FIG. 1) which teaches the concept of having a common key store in an integrated circuit and/or in a monolithic device).*

20. Applicant argues that: "In most of the embodiments of Ducharme, the store equated with the common key store (memory 130) is a read-only memory and, therefore, has no route to placing a common key in the store, at least during normal use."

It should be noted that Ducharme teaches a encryption key registry which store key and it should be understood that registry is not a read-only memory which can stores data on a permanent basis (col. 2, lines 18-50, col. 3, lines 5-61, col. 4, lines 35-

47, col. 5, lines 19-35, col. 7, lines 58-67 and col. 8, lines 20-65; *it should be noted that Ducharme discloses a encryption key register 130 (FIG. 1) which teaches the concept of having a common key store in an integrated circuit and/or in a monolithic device*).

21. Applicant argues that: "Ducharme teaches that the key is generated within the monolithic circuit without being encrypted"

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Mills teaches other aspect of claimed invention such as how the keys are broadcasted (e.g. see, e.g. col. 11, lines 9-50).

Conclusion

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435